TRIPWIRE NERC SOLUTION SUITE

TAILORED SUITE OF PRODUCTS AND SERVICES TO AUTOMATE NERC CIP COMPLIANCE

> *"We've been able to stay focused on our mission of delivering reliable energy and still achieve our NERC CIP compliance requirements through the use of Tripwire's tailored NERC CIP Solution Suite. They are committed to understanding our issues and have saved us incredible amounts of time and real dollars as well."*
>
> **SOUTHWESTERN US ENERGY HOLDING COMPANY**

The North American Electric Reliability Corporation (NERC) maintains comprehensive reliability standards that define requirements for planning and operating the bulk electric system. Among these are 10 Critical Infrastructure Protection (CIP) Cyber Security Standards, which specify a minimum set of controls and processes for power generation and transmission companies to follow to ensure the reliability and security of the North American power grid.

These standards have been undergoing multiple revisions since their original introduction in 2008, and with the recent approval of CIP v5, NERC registered entities must determine how to best address the standard's frequently changing, increasingly prescriptive requirements. They need to be audit-ready at all times, no matter what version of the standard is in play. At the same time, the time-consuming, complex task of meeting NERC CIP compliance must not distract IT and operations staff from their primary focus: ensuring the reliability of the bulk electric system. The Tripwire NERC Solution Suite helps meet those demands with a tailored package of products and expertise designed to help electric utility companies automate and simplify NERC CIP compliance.

The top priority for those working with industrial control systems in the power industry has always been reliability. However, with cyber incidents on the

rise, the security of IT assets on which the bulk electricity system depends has become critical.

NERC CIP compliance requires registered entities to establish a set of controls and processes, continuously monitor those processes, and produce detailed evidence of these activities in an audit. Doing this can be complex and time-consuming (especially when done manually), and can quickly overwhelm IT and operations departments. But the cost of findings in an audit can be significant—in recent years, non-compliant registered entities have been assessed fines of totalling over $150 million. Equally concerning is that such non-compliance leaves utilities more exposed to cyber attacks and more likely to experience service disruptions—putting the entire power grid at risk.

The Tripwire NERC Solution Suite helps registered entities pass their audit today and be more prepared for tomorrow's. It lets them do this efficiently and with greater confidence that they are protecting their assets and maintaining reliability.

With the Tripwire NERC Solution Suite, power companies can achieve and maintain NERC compliance through:

- **Continuous Monitoring** to continuously collect detailed status information on all your critical cyber assets and immediately detect any changes;
- **Automated Assessment** to automatically aggregate and analyze your security data and alert on suspicious events or modifications that impact your compliance status;
- **Asset Tagging Management Framework** to flexibly and easily tag your critical assets based on Impact Rating, associated BES System, Role, Owner, Location, etc., and have them automatically inherit the appropriate security control and classifications (e.g. daily vs. monthly scans, patch validation workflows, account enforcement policies, etc.); and
- **Audit-ready Evidence of Compliance** to quickly generate reports and dashboards that fully document, by CIP requirement, your compliance with security controls and processes.

Plus, they get these capabilities paired with the cumulative experience of Tripwire's system engineers and professional services consultants who have helped over 100 power companies address NERC CIP compliance over the past four years.

TRIPWIRE NERC CIP COVERAGE

Solutions will be tailored to meet the exact needs of each customer, helping to meet as few as one to as many as 19 of the CIPv5 requirements (and 24 of the v3 requirements). Many of the CIP requirements are administrative or pertain to physical controls, but of those requirements involving technical controls, the Tripwire NERC Solution Suite can help automate almost all of them.

TRIPWIRE COVERAGE OF NERC CIPv5 REQUIREMENTS

10 Standards | 32 Requirements

CIP-002 BES CYBER SYSTEM IDENTIFICATION AND CATEGORIZATION	CIP-003 SECURITY MANAGEMENT CONTROLS	CIP-004 TRAINING AND PERSONNEL SECURITY	CIP-005 ELECTRONIC SECURITY PERIMETER	CIP-006 PHYSICAL SECURITY OF BES CYBER SYSTEMS	CIP-007 SYSTEMS SECURITY MANAGEMENT	CIP-008 INCIDENT REPORTING AND RESPONSE PLANNING	CIP-009 RECOVERY PLANS FOR BES CYBER SYSTEMS	CIP-010 CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS	CIP-011 INFORMATION PROTECTION
1. BES CYBER SYSTEM IDENTIFICATION	1. CYBER SECURITY POLICY FOR HIGH/MEDIUM SYSTEMS	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	1. PHYSICAL SECURITY PLAN	1. PORTS AND SERVICES	1. CYBER SECURITY INCIDENT RESPONSE PLAN	1. RECOVERY PLAN SPECIFICATIONS	1. CONFIGURATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	2. TRAINING	2. INTERACTIVE REMOTE ACCESS MANAGEMENT	2. VISITOR CONTROL PROGRAM	2. SECURITY PATCH MANAGEMENT	2. CYBER SECURITY INCIDENT RESPONSE PLAN IMPLEMENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTATION AND TESTING	2. CONFIGURATION MONITORING	2. BES CYBER ASSET REUSE AND DISPOSAL
	3. IDENTIFICATION OF SENIOR MANAGER	3. PERSONNEL RISK ASSESSMENT PROGRAM		3. MAINTENANCE AND TESTING PROGRAM	3. MALICIOUS CODE PREVENTION	3. CYBER SECURITY INCIDENT RESPONSE PLAN REVIEW, UPDATE, COMMUNICATION	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATION	3. VULNERABILITY ASSESSMENTS	
	4. DELEGATION OF AUTHORITY	4. ACCESS MANAGEMENT PROGRAM			4. SECURITY EVENT MONITORING				
		5. ACCESS REVOCATION PROGRAM			5. SYSTEM ACCESS CONTROLS				

FIG. 1 *The Tripwire NERC Solution Suite helps electric utility companies meet 19 of the 32 requirements contained in the 10 standards.*

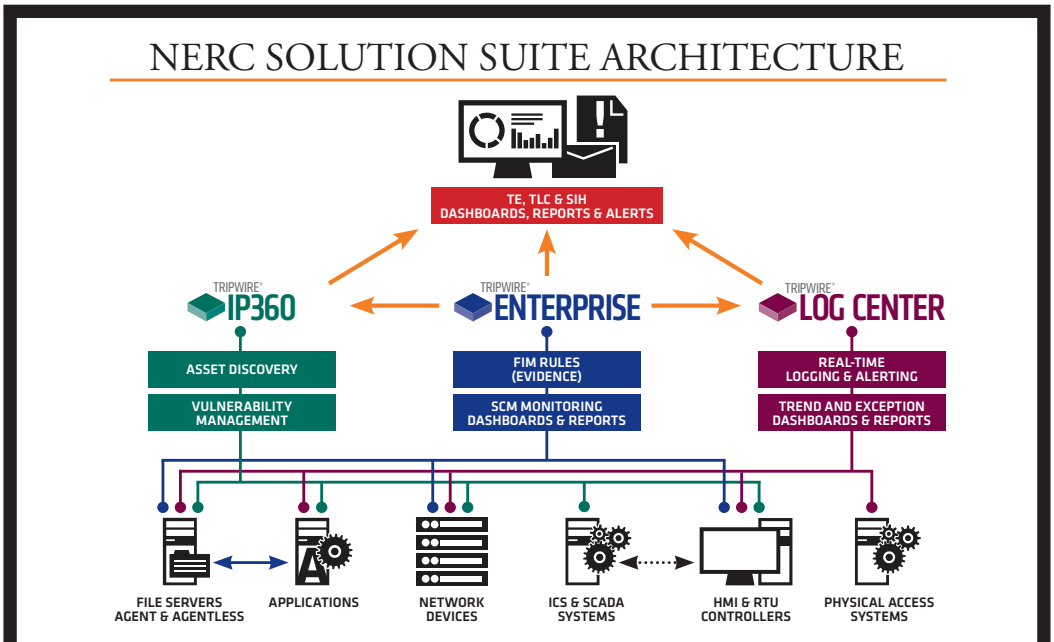


FIG. 2 *The Tripwire NERC Solution Suite combines standard Tripwire products, plus NERC-specific extensions and tailored content.*

WHAT IS THE TRIPWIRE NERC SOLUTION SUITE?

The Tripwire NERC Solution Suite offers electric utilities a tailored package that helps automate and simplify NERC CIP compliance. It uses standard Tripwire products and supplements them with NERC-specific extensions and content that includes tailored reports, dashboards, correlation rules, scripts, utilities, tools and templates. NERC-experienced consultants then deliver process assistance and training to help the power company reduce the amount of time and effort required to achieve NERC CIP compliance.

While the complete NERC Solution Suite uses the functionality of Tripwire Enterprise, Tripwire Log Center and Tripwire IP360, the customer does not have to have all Tripwire products to benefit from the solution—both Tripwire Enterprise and Tripwire IP360 can integrate with other log management and SIEM products. An initial assessment helps tailor each implementation to the needs of the individual customer, including appropriate Tripwire products as well as interfacing to other technologies.

TRIPWIRE NERC SOLUTION SUITE COMPONENTS: TRIPWIRE ENTERPRISE

Tripwire Enterprise offers an industry-leading security configuration management (SCM) solution that automatically assesses, detects and assists in correcting file and configuration changes across the IT infrastructure to ensure NERC compliance. With Tripwire Enterprise, customers receive:

- **Comprehensive change auditing** that provides proof of changes with before and after images.
- **Continuous monitoring** of configuration hardening requirements to achieve and maintain compliance.
- **Customized reports and dashboards** grouped by NERC CIP requirement to document compliance and provide operational control.
- **Whitelist profiling** that automates validation of system settings, including ports/services, local user accounts and software versions, on a per-device basis.
- **Broad support for critical cyber assets**, including file systems, applications, network devices, SCADA devices, HMI/RTU controllers and badge entry systems.

TRIPWIRE NERC SOLUTION SUITE COMPONENTS: TRIPWIRE LOG CENTER

Tripwire Log Center is a complete log and event management solution that provides efficient log processing and sophisticated event analysis to meet NERC log management requirements while providing access to data that helps organizations identify security

events of interest and determine their root cause. With Tripwire Log Center, customers receive:

- **Complete audit log capture** and retention of all log events.
- **Normalization and correlation rules** to detect and alert on abnormal behavior.
- **Customized reports and dashboards** to document compliance and provide forensic analysis.

An advantage of using integrated Tripwire Enterprise and Tripwire Log Center solutions is they share data and components, providing a consistent view of your security posture that allows you to better identify the highest risk changes and events within your IT environment.

TRIPWIRE NERC SOLUTION SUITE COMPONENTS: TRIPWIRE IP360

Tripwire IP360 is a comprehensive vulnerability management solution that provides detailed assessments of a broad variety of asset classes in your environment and provides an ideal foundation for assessing every system on the network. With Tripwire IP360, customers receive:

- **Comprehensive asset discovery and profiling** of all network-connected assets.
- **Industry-leading vulnerability assessment** with coverage of the latest operating systems, applications and vulnerabilities.
- **Flexible risk-based reporting** across all levels of the enterprise.

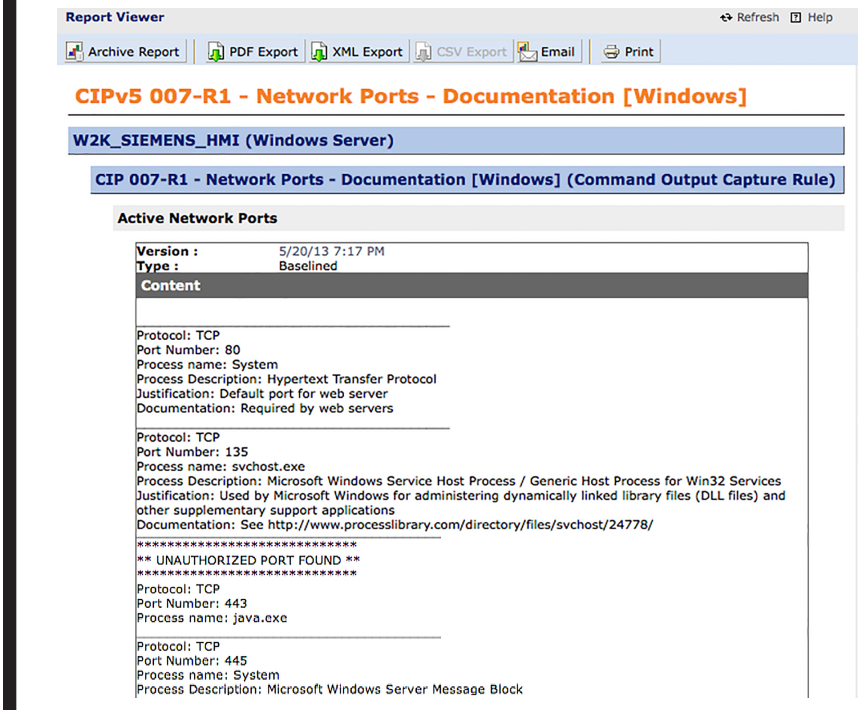
TRIPWIRE NERC SOLUTION SUITE COMPONENTS: EXTENSIONS AND TAILORED CONTENT

The Tripwire NERC Solution Suite offers different NERC-specific extensions and content based on the customer's specific needs and the Tripwire products in use.

TRIPWIRE ENTERPRISE EXTENSIONS AND CONTENT

- **NERC configuration policy tests** provide continuous awareness of compliance across a broad range of CIP requirements and significantly reduce the burden of preparing for an audit. They also provide relevant security and configuration information to operations staff—for example, where

FIG. 3 *The Tripwire Enterprise NERC CIP dashboard provides a quick view of overall compliance status*



◆ **FIG. 4** *Tripwire Enterprise element content reports meet the CIP 007 R1 requirement to document the current status and justification for all ports and services on all BES Cyber Assets.*

BENEFITS OF TRIPWIRE NERC SOLUTION SUITE

◆ The Tripwire NERC Solution Suite enables electric utility companies to be audit-ready for NERC CIP v3 as well as v5.

- » **Increase NERC CIP Audit readiness**
- » **Provide audit-ready reporting**
- » **Automate compliance monitoring**
- » **Automate discovery and management of Cyber Assets**
- » **Reduce Cyber Asset attack surface**
- » **Achieve compliance beyond NERC CIP, to include PCI, HIPAA, SOX, etc.**
- » **Customize for varying levels of NERC CIP readiness**

antivirus software or system logging have been disabled.

- » **Tailored monitoring rules**, which are selected based on the customer, provide the evidence to auditors that the standard requires—for example, active users and groups, installed applications, and password policies. Tailored rules also help system administrators by providing general operational awareness information such as service state, password aging and antivirus status.
- » **Whitelist profiling** lets the customer define a set of expected system values and compare those to the current state, defined on a per host basis. For example, this could let the customer ensure that only authorized network ports are in use on specific systems or that revoked user accounts are removed from critical systems.
- » **Customized dashboards and reports** consolidate system information to provide the evidence required by auditors, while also giving the operations staff an overall awareness of the security and operations in their environment. High-level custom dashboards can be created based on the particular role of a team member (for example, compliance, security or operations).

TRIPWIRE LOG CENTER EXTENSIONS AND CONTENT

- » **Tailored logging and correlation rules.** NERC-experienced consultants help tailor audit normalization rules to effectively and reliably collect and process log events for BES Cyber Assets such as SCADA devices and physical entry systems. This provides visibility across the environment and addresses security goals. For example, rules could be developed to ensure that revoked or unprivileged user accounts are no longer in use or that provide effective logging retention across all systems.
- » **Customized dashboards and reports** can provide consolidated evidence for auditors while giving the operations staff a complete view of security and operations in their environment. High-level dashboards can also be created that present salient information to security, compliance and operations teams.

TRIPWIRE NERC SOLUTION SUITE COMPONENTS: NERC-EXPERIENCED CONSULTANTS

To ensure effective tailoring and deployment of Tripwire products to the specific environment for the electric utility company, Tripwire's NERC solution provides consulting from Tripwire

Professional Services. These NERC-experienced consultants will work with an organization to:

- **Develop best practices** around discovery methods and discuss the company's classification/taxonomy process to ensure that Tripwire accurately reflects how they view and manage their business.
- **Review the reports and dashboards** that auditors will require and tailor monitoring rules and reports that operators, managers, executives and compliance program staff will use to manage and report on security compliance programs.
- **Provide specialized training** for staff on using Tripwire products to perform forensic analysis and determining the risks associated with hacking or a breach. This permits companies to perform more comprehensive root cause analysis, which in turn helps with compliance and remediation.

The table below provides specific details about how the Tripwire NERC Solution Suite's combination of products, tailored extensions and NERC-experienced consultants can address 19 of the 32 NERC CIPv5 requirements.

CIP-002-5: Cyber Security — BES Cyber System Identification and Categorization		
CIP-002 R1: BES Cyber System Identification		Tripwire IP360 combined with professional services use of Tripwire discovery tools can help identify and track the critical cyber assets that are in scope. Tripwire IP360 can discover all assets in assigned IP scope using TCP and UDP protocols. Discovery of all assets allows for further classification and interegation.
CIP-003-5: Cyber Security — Security Management Controls		
CIP-003 R2: Cyber Security Policy for Low Systems	**R2.3**	Tripwire validates and monitors security settings and related configurations to ensure that monitoring of dial-up services and features has been implemented.
	R2.4	Tripwire reports can provide excellent forensic details to assist in the investigation/ analysis of an Incident or in the preparation/evaluation of an IOC report.
CIP-004-5 Cyber Security — Training & Personnel Security		
CIP-004 R4: Access Management Program		Tripwire Enterprise and Log Center is used to verify account and access control settings on systems and networks via logs and configuration changes.
	R4.3	Tripwire's FIM whitelist profiler extension can verify only approved accounts exist on systems, as codified in an authorized user whitelist.
CIP-004 R5: Access Revocation Program	**R5.4**	Standard monitoring access logs comes out of the box with Tripwire Log Center; access controls are monitored by TE, and tailored rules can be created to search for access control logs that match lists of former employees to validate that access and activity by the former employees has been stopped. Tripwire's FIM whitelist profiler extension can verify only approved accounts exist on systems, as codified in an authorized user whitelist.
	R5.5	Tripwire can help ensure that shared accounts have suitable controls, and that passwords have been changed according to stated policies.
CIP-005-5 Cyber Security — Electronic Security Perimeter(s)		
CIP-005 R1: Electronic Security Perimeter	**R1.1**	Tripwire IP360 combined with professional services use of Tripwire discovery tools can help identify and track the cyber assets that are in scope.
CIP-005 R2: Interactive Remote Access Management		Tripwire Change Auditing and Configuration Assessment/reporting will track settings associated with authenticated access control for remote use.
	R2.2	Tripwire validates and monitors security settings and configurations made to ensure strong authentication by external interactive users.
CIP-006-5 Cyber Security — Physical Security of BES Cyber Systems		
CIP-006 R1: Physical Security Plan	**R1.4**	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems through automated collection and analysis of these device logs by Tripwire Log Center.
	R1.5	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems by analyzing the logs collected, utilizing custom correlation rules to alert on unauthorized access attempts.
	R1.6	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems through automated collection and analysis of these device logs by Tripwire Log Center.
	R1.7	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems by analyzing the logs collected, utilizing custom correlation rules to alert on unauthorized access attempts.
CIP-006 R2: Visitor Control Program	**R2.3**	Log retention for the required periods can be assured through Tripwire's log management and archiving capabilities.

CIP-007-5 Cyber Security — Systems Security Management		
CIP-007 R1: Ports and Services	Tripwire's FIM whitelist profiler extension can monitor ports and services and compare current state against a tailored set of customer-specific approved port and services, alerting when monitoring detects a variance.	
	R1.1	Tripwire's FIM whitelist profiler extension can monitor ports and services and compare current state against a tailored set of customer-specific approved port and services, alerting when monitoring detects a variance.
	R1.2	Tripwire can detect whether removeable media has been connected to a monitored system, providing timely alerting to potential violations.
CIP-007 R2: Security Patch Management	Tripwire's FIM whitelist profiler extension can identify software versions and installed patches and compare current state against a tailored set of customer-specific approved software versions and patches, alerting when there is a variance on specific BCA's.	
	R2.2	IP360's vulnerability assessment capabilities can identify any necessary patches that should be installed on a broad range of BCA systems based on vendor recommendations. The vulnerability database is typically updated every week.
	R2.3	Tripwire detects when patches are implemented and will record this information for later review and analysis.
CIP-007 R3: Malicious Code Prevention	Tripwire can scan for anti-virus and malware products installed through tailored change auditing rules. Logs can be watched to find specific malware events and allow the Tripwire operator to examine the device for incident information.	
	R3.1	Tripwire's FIM monitoring can detect the introduction of unapproved/unauthorized files on a given system.
	R3.3	Tripwire checks for security settings and configurations to validate anti-virus and malware prevention is enabled and updated appropriately.
CIP-007 R4: Security Event Monitoring	Tripwire can scan logs for account management activity and configuration settings for changes to account privilege, alerting as appropriate.	
	R4.1	Tripwire Log Center rules can capture successful and unsuccessful logins for all monitored hosts, and provide alerting as desired.
	R4.2	Tripwire Log Center rules can detect and alert when a BCA stops logging activity, thus providing alerting on continuous 24x7 basis.
	R4.3	Log retention for the required periods can be assured through Tripwire's log management and archiving capabilities.
	R4.4	Log retention for the required periods can be assured through Tripwire's log management and archiving capabilities.
CIP-007 R5: System Access Controls	Tripwire can scan logs for account management activity and configuration settings for changes to account privilege, alerting as appropriate.	
	R5.1	Tripwire can scan logs for account management activity and configuration settings to ensure authentication is enforced, alerting as appropriate.
	R5.2	Tripwire's FIM whitelist profiler extension can verify only approved accounts exist on systems, as codified in an authorized user whitelist.
	R5.4	Tripwire can ensure that default accounts are disabled and/or passwords are changed where required, and activity logging can provide alerting on inappropriate use of such accounts.
	R5.5	Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements.
	R5.6	Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements.
	R5.7	Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements, and provide alerting when success/failure thresholds are exceeded.
CIP-008-5 Cyber Security — Incident Reporting and Response Planning		
CIP-008 R1: Cyber Security Incident Response Plan	**R1.2**	Tripwire reporting on logs, events, configuration and change detection would help to create IOC reports that could be part of an ISAC response document.
CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Systems		
CIP-009 R1: Recovery Plan Specifications	**R1.3**	Tripwire products can be customized to create baselines for products and devices configuration. These may be called for and used for recovery steps taken after incidents of system attack or failure.
	R1.4	Tripwire products can be customized to create baselines for products and devices configuration. These may be called for and used for recovery steps taken after incidents of system attack or failure.
	R1.5	Tripwire products can be used to collect and aggregate logs and event information from a variety of sources. This information can be stored and later used for recovery steps taken after incidents of system attack or failure.
CIP-009 R2: Recovery Plan Implementation and Testing	Tripwire products can be customized to create baselines for products and devices configuration. These may be called for and used for recovery steps taken after incidents of system attack or failure.	
	R2.2	Tripwire products can be used to collect baselines, logs and event information from a variety of sources. This information can be stored and later used for recovery steps taken after incidents of system attack or failure.

CIP-010-1 Cyber Security — Configuration Change Management and Vulnerability Assessments		
CIP-010 R1: Configuration Change Management	Tripwire Configuration Assessment Policy and Change audit features can address the creation of a baseline configuration of computer systems and alert and report on change—supporting the process of formal change control and testing.	
	R1.1	Tripwire Configuration Assessment Policy and Change audit features can address the creation of a baseline configuration of computer systems and alert and report on change—supporting the process of formal change control and testing.
	R1.2	Tripwire supports the tracking and authorization of change to system baseline and configurations—following the process defined by NIST for POA&M reporting
	R1.3	Tripwire supports the tracking and authorization of change to system baseline and configurations—following the process defined by NIST for POA&M reporting
	R1.4	Tripwire reports on security controls deployed, configured and operational status. This reporting will support this requirement.
	R1.5	Tripwire baseline comparison operations can verify that a given test environment accurately reflects the production systems.
CIP-010 R2: Configuration Monitoring	Tripwire's core functionality offers exceptional change detection and investigation capabilities.	
	R2.1	Tripwire Enterprise's core functionality offers exceptional change detection and investigation capabilities.
CIP-010 R3: Vulnerability Assessments	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types.	
	R3.1	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types.
	R3.2	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types. Controls exist to minimize the potential for adverse effects during a scan.
	R3.3	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types. Controls exist to minimize the potential for adverse effects during a scan. Tripwire Enterprise can be used to ensure the test environment is equivalent to the target BCA.
	R3.4	SIH reporting can offer very capable analysis and mitigation reports. Can be tailored based on mitigation tools available.
CIP-011-1 Cyber Security — Information Protection		
CIP-011 R1: Information Protection	Tripwire can be used to 1) generate evidence for audit of BCA for file system access controls, and 2) identify files used for evidence of compliance, monitoring them for change and retension (according to requirements and reported for auditors and compliance officials.)	
	R1.2	Tripwire Change Auditing feature can be custom configured to assess if an application or operating system is configured for secure data transmission, storage or event logging—itself logging when these settings are changed or suppressed. This feature could support the appropriate management of BES information protection.

RELY ON TRIPWIRE FOR NERC CIP COMPLIANCE

As a recognized leader in solutions for IT security and compliance, Tripwire has significant experience helping customers automate compliance for numerous standards across almost any device, platform and system. Tripwire has helped registered entities achieve and maintain NERC compliance since 2008—experience that has allowed Tripwire to develop a team of consultants well versed in NERC compliance and the product extensions and NERC-specific content now embedded in the NERC Solution Suite.

With the Tripwire NERC Solution Suite, electric utilities have a comprehensive solution—from products, to customized extensions and content and expert consulting—to help them automate and simplify NERC compliance. By meeting NERC compliance, these companies secure their IT/OT systems against inadvertent misuse and intentional, malicious attacks. In turn, these secure systems help these companies ensure the reliability of North America's bulk electric system.

◆ With the NERC Solution Suite, power companies can automate and simplify their NERC compliance demands by taking advantage of Tripwire's:

- » Asset discovery
- » Continuous monitoring
- » Automated assessment
- » Audit-ready evidence
- » NERC-experienced consultants

tripwire®

◆ Tripwire is a leading global provider of risk-based security and compliance management solutions that enable organizations to effectively connect security to the business. Tripwire delivers foundational security controls like security configuration management, file integrity monitoring, log and event management, vulnerability management, and security business intelligence with performance reporting and visualization. ◆

LEARN MORE AT WWW.TRIPWIRE.COM OR FOLLOW US @TRIPWIREINC ON TWITTER.

SBNRCS2t 201402